BRIEFING NOTE

FINANCIAL CRIME IN 2021:

NO TIME FOR COMPLACENCY

JANUARY 2021

INSIGHT | INTELLIGENCE | INNOVATION

www.crime.financial

THEMIS

INTRODUCTION

2020 was a challenging year in a variety of ways, financial crime being no exception. The COVID-19 pandemic found governments, economies and regulators unprepared for a rapid, large-scale response to a sudden new global threat. And, while authorities rushed to stabilise markets and guarantee consumer protection, criminals sought out novel forms of illicit activity.

69% of respondents to the Themis Financial Crime Survey 2020 thought there was an increased threat of financial crime by the end of the year, and rightfully so; the pandemic and associated rise in unemployment forced many people into highly precarious economic situations, which criminals were quick to exploit. Additionally, the shift towards home working created new opportunities for online scams, whereas the speed and scale of mobilisation of government support programmes and stimulus packages led to a number of erroneous and fraudulent benefit claims.

In the meantime, businesses hurried to implement effective remote working arrangements, confronting difficult tasks like data storage and digital Know Your Customer (KYC) verification, which proved tempting prey for cyber criminals. Cases such as the Wirecard story and the FinCEN Files revelations, both legacies of previous years of wrongdoing and systemic flaws, also demanded the attention and resources of the financial services sector. Finally, many planned regulatory changes were temporarily postponed or reoriented, as regulators across jurisdictions shifted their short-term focus to providing pandemic relief to both firms and their customers.

As we enter into 2021, new directives and regulations add complexity to the fight against financial crime across all industries. Likewise, criminals are expected to elaborate new ways of conducting illicit business. With the pandemic still ravaging many parts of the world, intermittent lockdowns and resulting economic shockwaves, COVID-related crime will continue to evolve.

For instance, Interpol and other organisations have warned that the COVID-19 vaccine could easily become the target of criminal activity. Furthermore, in the United Kingdom, Brexit will imply a change in regulations, increased complexity in cooperation and information sharing, as well as new procedures that may be exploited by criminals. It is also important to look out for modern slavery practices throughout businesses operations and their supply chains, as more firms may be tempted to cut corners in terms of labour costs, leading to abuse and exploitation.

In this briefing note, we analyse upcoming trends in financial crime and consider key financial crime-related regulation that is expected in 2021. Forecasting upcoming threats is crucial as it enables us all to better defend ourselves against them.

FINANCIAL CRIME TRENDS: WHAT TO EXPECT IN 2021

1. Fraud is still a number one priority

The COVID-19 pandemic and associated economic downturn have led to a marked increase in several different types of fraud. In 2020, fraudsters took advantage of unprecedented new government stimulus packages and benefits by using stolen and synthetic identities. In early September 2020, HM Revenue & Customs (HMRC) estimated that up to 10% of Coronavirus Job Retention Scheme (also known as CJRS or furlough scheme) payments were made on the basis of incorrect and/or fraudulent claims.

A subsequent report in October 2020 showed that HMRC had received over 10,000 reports of suspected CJRS fraud via its hotline. With the pandemic still ravaging our economies, this trend is unlikely to decrease into the new year, and fraud continues to be amongst the crimes that worry businesses most, our Themis Financial Crime Survey 2020 reports.

The misuse of funds by organised crime groups may pose another challenge. As of June 2020, the International Monetary Fund (IMF) estimated that approximately USD 11 trillion had been allocated globally in fiscal support to the COVID-19 response, representing a significant opportunity for criminals to embezzle money. Corruption risks in emergency funding have arisen in previous pandemics; for instance, the United Nations Office on Drugs and Crime (UNODC) reports that, following the Ebola crisis, nearly USD 6 million in payments and disbursements from Sierra Leone government's Ebola-directed accounts went undocumented or were only partly documented. Related instances of fraud and corruption were also noted - and this trend may come to the fore again in light of huge COVID-19 emergency funding.

Closer to home, the European Union is especially at risk. EU funds have always been a lucrative target for financial criminals and, with EUR 1.8 trillion put at member states' disposal to rebuild a post-COVID-19 Europe, authorities and financial institutions must take steps to ensure this money does not fall into the wrong hands.

Interpol, Europol and UNODC have also warned of the involvement of organised crime groups in the manufacturing of and trafficking in falsified vaccines, as well as the production of substandard vaccines. Given the urgent global demand for a vaccine that should help us ease out of the COVID-19 crisis, there is a risk of counterfeit products entering the pharmaceutical market. The UNODC also anticipates instances of conflicts of interests, nepotism and corruption in the allocation of vaccines to priority groups, especially in light of limited supplies during the initial stages of deployment.

Throughout the pandemic, criminals have exploited the cyber vulnerabilities presented by remote working to access confidential data, making banking and pension fraud a worrying reality. Recognising the significant risk of harm in these particular markets, the UK's Financial Conduct Authority (FCA) has continued its ScamSmart campaign, focused on mitigating consumer harm arising from four types of fraud – pensions, investment, online fraud and loan fee fraud. The FCA foresees that criminals will target pension pots of all sizes throughout 2021, exploiting the pandemic-related financial difficulties of many pensioners and promoting fraudulent pension plans with fake high returns.

Banking fraud, which involves the fraudulent use of an individual's banking details, had risen by 33 percent across all financial services in the UK by April 2020 and is expected to continue challenging financial institutions in 2021. According to market research organisation Forrester, "2021 will reveal the high number of fraudulent COVID-19 loans; while governments have often underwritten these, they will tarnish banks' reputations." [1]

Meanwhile, the FCA also warns that online transactions and online shopping have increased over the past year - and so has the associated risk of theft of personal data by criminals seeking to withdraw cash or buy goods remotely. In the UK, since March 2020, when the country first went into lockdown, about 96 percent of adults have purchased an item online. Correspondingly, online fraud has increased in number and type. In 2021, consumers must continue to remain vigilant when conducting online shopping, as fraudsters tend to hide their identity and target many victims at the same time.

1. Forrester, "The European Predictions 2021 Resources Finder" https://go.forrester.com/europe- predictions/

2. Watch out for cyber crime

The shift towards online transactions and cloud data storage is likely to result in an increase in fraud orchestrated through the theft of personal information. The current remote working environment also complicates customer due diligence and KYC operations, and contributes to delays in reviewing transaction monitoring alerts, giving fraudsters more freedom to move. Breaches may originate from different sources, the most common being cyber criminals exploiting either third party suppliers who do not have up-to-date cyber security protocols or weak servers of company employees working from home. Much of the fraud that we are likely to see in 2021 will be facilitated by cyber crime. 2020 has weakened the security of some businesses due to the hasty deployment of remote working solutions; the COVID-19 pandemic has greatly accelerated many organisations' digital transition, but often at a pace that did not allow for the proper training of employees or implementation of cyber security controls.

With a vaccine in sight, many businesses will be facing decisions about whether to stage a comprehensive return to the office. In the meantime, they still represent easy prey for cyber criminals. Coming back to the office will also pose a cyber security challenge, as firms will have to manage all the data stored in the cloud that was accessible via vulnerable remote connections and transfer it from one server to another, creating loopholes for criminals to exploit.

Furthermore, both remote working and transition back to the office represent an opportunity for new forms of cyber crime, including targeted ransomware campaigns and distributed denial of service (DDoS) attacks. In 2020, the APAC region was most affected by ransomware, with the highest average ransom payout reaching USD 1.18 million, followed by EMEA at USD 1.06 million and the United States at USD 0.99 million. In 2021, online extortion practices are likely to become more widespread, facilitated by the unprecedented access that ransomware gangs have to employees working remotely. These groups have developed new open-source tools, actively exploiting corporate email systems and using extortion techniques to scare victims into paying ransom. Approximately 31 percent of respondents to a recent Themis survey were concerned by the specific threat posed by malicious documents in 2020, and reported an increase in these concerns as a result of remote working.

Researchers argue that state-sponsored cyber attacks are likely to be another big threat this year. In 2020, we already saw state-sponsored hackers from China, Russia, Iran and North Korea targeting vaccine developers with attacks such as password spraying or spear phishing. Furthermore, several governments and firms in different sectors ranging from consulting to energy were attacked in North America, Europe, Asia and the Middle East - the latest one being the U.S. Departments of Homeland Security, Treasury and Commerce. The New York Times reports that, following this hack, the chance of further, widespread intrusion into government and corporate networks has increased. Moreover, state hackers are continuing to undermine efforts to supply the vaccine. IBM reports that since September 2020, suspected state-sponsored hackers have attempted to target the Cold Chain Equipment Optimisation Platform (CCEOP) of Gavi, the international vaccine alliance, which helps distribute vaccines to some of the world's poorest regions. This threat is likely to increase in 2021 and necessitates vigilance and tight cyber security across both governmental agencies and target industries.

3. Money laundering

If 2020 was the year of fraud, 2021 will see an upsurge in the laundering of fraudulently acquired COVID-19 government benefits and support funds into the banking system. 46 percent of respondents to the Themis Financial Crime Survey 2020 reported exposure to money laundering - a trend that is likely to increase if no measures are put in place.

Defence Against Money Laundering (DAML) Suspicious Activity Reports are already on the rise in the UK, an early indicator that the laundering of COVID-19 fraud proceeds has already started. Lockdown has had consequences on the ability of money launderers to move cash across borders, prompting them to find alternative processes such as crypto asset exploitation or trade-based money laundering. More attention should, therefore, be paid to these types of laundering methods. Criminals have also used the enduring pandemic as a justification for unusual account activity and suspicious money transactions, criminal behaviours that are likely to continue into the new year as lockdowns and stimulus packages are extended.

Furthermore, as we enter into 2021, criminals may seek alternative locations and sources through which to launder the proceeds of their criminal activities. Following recommendations made at the October 2020 G20 Summit to enhance transparency in beneficial ownership, scrutiny of corporate secrecy is expected to intensify this year. However, the degree of scrutiny may vary from one jurisdiction to another: as a consequence, increased attention should be paid to flows of money to and from tax havens or high risk jurisdictions, which is where criminals may increasingly focus their activities.

4. Brexit

In the UK, Brexit could also represent a lucrative opportunity for criminals, who may take advantage of possible Brexit-related shortages of food, fuel and medicine. Organised crime groups could resort to acquisitive crime and exploit the increased demand for these goods to create hidden markets for items held up in ports.

Even though a zero tariff, zero quota trade deal was agreed by the UK and the European Union on Christmas Eve 2020, trade will not run as smoothly as before. Businesses will need to file new paperwork and financial services firms will lose their passport to offer services across the EU. Indeed, the National Audit Office (NAO) estimates that HMRC could see an annual increase of 220 million customs declarations, overwhelming law enforcement agencies and leaving the door open for organised crime groups to illegally traffic goods into the UK. Increased paperwork may also facilitate trade-based money laundering, including via over/under invoicing and shipments which misrepresent or falsely describe goods.

According to UK law enforcement authorities, the major adverse impact of Brexit will relate to information sharing and cooperation between UK and European Union authorities, hindering both sides' ability to stop international offenders in their tracks. Since 1st January 2021, the UK's National Crime Agency has not had access to FIU.net, a decentralised database that allows European Financial Intelligence Units to share and request information from other EU jurisdictions when addressing Suspicious Activity Reports (SARs). As a result, monitoring of international financial flows and money laundering prevention efforts will be impeded.

Another important tool that the UK will lose access to is the European Arrest Warrant, a framework designed to facilitate the transfer of individuals across EU member states' borders to either face prosecution or serve a prison sentence. This warrant has proven incredibly useful in terrorism and organised crime investigations to date. Europol does have cooperation arrangements in place with some non-EU members such as the United States, and a similar framework between the EU and UK could help secure continuity in law enforcement efforts. The Brexit Treaty includes a commitment by the EU and UK to uphold high data protection standards, as well as to ensure cooperation. However, additional effort on both sides will be required to guarantee that cross-border crime prevention and law enforcement run as smoothly as in the pre-Brexit era.

FINANCIAL CRIME REGULATION IN 2021

2020 was a difficult year for regulators, as they had to act to protect consumers during the pandemic without losing sight of the priorities they had set before COVID-19 materialised. At the same time, the FinCEN File revelations and other important cases such as the Wirecard story increased pressure on regulators to improve processes and credibility.

Pandemic-related mitigation and relief efforts will remain at the top of regulators' agendas in 2021. However, the new year is expected to provide more scope for a parallel regulatory focus on medium and longer term priorities.

For instance, 2021 represents an opportunity for regulators to implement new technology such as artificial intelligence to increase their monitoring, detection and information sharing capabilities - and to encourage businesses to do so too. Remote working has already forced many businesses to accelerate their implementation of digital solutions. Although this has created cyber vulnerabilities that criminals have been quick to exploit, it has also given impetus to regulators to encourage the responsible use of technology to meet financial crime obligations during the pandemic. We are likely to see a continuation of this trend in 2021, as anticipated by the FCA's 2020/2021 Business Plan, which promotes technology as a way to reduce the burden of regulatory reporting on firms.

The Business Plan outlines five medium-term priorities for the FCA. These focus on protecting consumers and minimising market harm, including in the spheres of investment, credit and payments. This year, the FCA is also set to accelerate its own internal transformation via a simplification of processes and enlargement of its regulatory toolkit.

Financial crime features in the Business Plan as a key cross-cutting area of FCA work, with the organisation seeking to ensure that all regulated firms implement effective systems and controls to detect and disrupt criminal activity, including fraud. In 2021, the FCA is also expected to publish its final rules on extending the annual financial crime reporting obligation to more firms. Furthermore, the regulator is set to continue its work on market manipulation and misleading statement cases. For instance, UK branches of firms from the European Economic Area will be required to file Suspicious Transaction and Order Reports (STORs) to the FCA going forward, regardless of any existing obligations to report STORs to their home state regulator.

With Brexit now concluded, the UK will adopt the remaining provisions of the Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020, which will work in conjunction with aspects of the EU's 5th Anti-Money Laundering Directive (AMLD) relating to money laundering and terrorist financing, in particular surrounding the registration of trusts and beneficial ownership. The UK deemed it unnecessary to implement the EU's 6th AMLD on the basis that stronger AML and CTF measures were already in place in its own national provisions.

As part of the Brexit transition, the British government has also been publishing a range of sanctions-related instruments covering different country and activity-based sanctions programmes that derive from European Union law. However, in the first quarter of the new year, we should expect increased regulatory divergence between the EU and UK, especially following the European Commission's anticipated publication of adoption plans for a comprehensive bloc-wide AML/CTF policy, outlined below.

While pre-existing AML/CTF provisions are covered by the Brexit deal, financial services are not. The EU and UK are aiming to agree to a Memorandum of Understanding establishing a framework for regulatory cooperation on financial services by March 2021. However, the scope of this framework remains uncertain, especially as British Prime Minister Boris Johnson has said he intends to use the UK's new post-Brexit regulatory freedom to diverge from the EU's rules regarding financial services.

In the European Union, member states are required to implement regulations related to the new 6AMLD by June 2021. The new year will also see the bloc's "action plan for a comprehensive Union policy on preventing money laundering and terrorism financing" hit the ground. According to this plan, the EU is to harmonise its AML framework by implementing a single AML rulebook in the first quarter of 2021. A new EU-level AML/CTF supervisor and a new EU coordination and support mechanism for national financial intelligence units are also envisaged. Finally, European efforts to harmonise the definition of money laundering, strengthen bloc-wide AML capabilities and facilitate better information sharing will continue into 2021.

A similar focus on information sharing is expected in the United States, where FinCEN recently published guidance encouraging financial institutions to participate in information sharing programmes. The September 2020 FInCEN leak highlighted flaws in the current system, with banks filing very high volumes of often incomplete Suspicious Activity Reports and thus impeding effective response on the part of regulators. Following this leak, FinCEN issued rules that expand the anti-money laundering obligations of financial institutions under the Bank Secrecy Act, and put forward a proposed Advance Notice of Proposed Rulemaking (ANPRM) to strengthen the national AML regime. In 2021, we will see the further development of these initiatives.

Many governments are also expected to focus on ultimate beneficial ownership (UBO) verification and corporate transparency over the upcoming year. For instance, the UK's Crown Dependencies and inhabited Overseas Territories recently committed to introducing publicly accessible company registers. In 2021, the British government is likely to implement a new beneficial ownership register of foreign entities that own UK property, as outlined in the draft Registration of Overseas Entities Bill, which was largely designed to prevent money laundering in the UK's property sector.

CONCLUSION

In 2021, we will see a continuation of many of the trends fostered by the COVID-19 pandemic. Whilst we adapt to new ways of conducting business, criminals develop innovative ways to exploit both pre-existing and new vulnerabilities.

Since an imminent, large-scale return to the office still looks unlikely in many parts of the world, it is up to financial institutions, businesses and regulators to harness the benefits of new technologies to protect themselves and their customers from cyber criminals - whilst also understanding associated risks. We are, for instance, likely to see a further increase in extortion practices such as ransomware, facilitated by the unprecedented access that criminal groups have to employees working remotely.

At the same time, as governments continue to provide their citizens with pandemic-related economic relief, they must remain vigilant and act quickly to detect and disrupt fraudulent activity. The risks of benefit, pension, banking and investment fraud remain particularly latent. Furthermore, although the rollout of the COVID-19 vaccine represents a clear beacon of hope for 2021, it also poses certain financial crime challenges, as criminals seek out weak links in supply chains, opportunities to counterfeit goods and signs of corruption in vaccine allocation processes.

Given these continued threats and liabilities, businesses must go the extra mile to ensure they have effective measures in place to deter and disrupt financial crime. Otherwise, they may fall victim to the ever-evolving and increasingly tech-enabled methods that criminals use to exploit vulnerabilities for their own gain.

Contact us if you would like any support fine-tuning your firm's anti-financial crime framework, culture or controls in 2021. We can employ our Themis AFC Rating to assess your existing risk management systems, and recommend improvements to rectify identified gaps. Watch a short video here to find out more. Businesses continue to be the first line of defence against financial crime so must equip themselves with the strongest possible armour to counter the emerging threats discussed in this briefing note.

Sandeep Sroa
Associate Director
sandeep.sroa@themisservices.co.uk
+44 (0) 7786 236 774

Henry Williams
Head of Investigations
henry.williams@themisservices.co.uk
+44 (0) 7780 746 290

Carel van Randwyck
CGO
carel.vanrandwyck@themisservices.co.uk
+44 (0) 7802 232681